REMARKS

Claims 1-22 are pending.

Claims 1-22 stand rejected.

Claims 3-17 and 18-22 have been amended.

Claims 1-22 are hereby submitted for review and consideration.

No new matter has been added.

In paragraph 1 of the Office Action, the Examiner has objected to the Abstract. Applicants have amended the Abstract according to the Examiner's suggestions and respectfully request that this objection be withdrawn.

In paragraph 4 of the Office Action, the Examiner has objected to claims 6, 7, 8, 9, 10, 15, 16, 20, 21 and 22 for containing minor informalities. Applicants have amended these claims accordingly and respectfully request that these rejections be withdrawn.

In paragraph 5 of the Office Action, the Examiner has indicated that if claims 5-10 are found allowable claims 11-16 would be objected to under 37 CFR 1.75 as being substantial duplicates thereof. Applicants have amended claims 11-16 accordingly and respectfully requests that this objection not be applied to claims 11-16.

In paragraph 7 of the Office Action, the Examiner has rejected claim 17 under 35 U.S.C. § 112 for containing subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventors had possession of the claimed invention. Applicants have amended claim 17 in accordance with the Examiner's suggestion and respectfully request that this rejection be withdrawn.

In paragraph 8 of the Office Action, the Examiner has rejected claim 21 under 35

U.S.C. § 112 for failing to comply with the written description requirement Applicants have amended claim 21 to include the limitation , "if the commonly operable encryption algorithm *does not* exist" rendering the latter limitation "reception side is *dis*abled" to be consistent with the specification, and thus respectfully request that this rejection be withdrawn.

In paragraph 10 of the Office Action, the Examiner has rejected claims 3-14, 16 and 20-22 under 35 U.S.C. § 112, for failing to particularly point out and distinctly claim the subject matter which the applicant regards as the invention. In particular in paragraphs 11-21, The Examiner has pointed out numerous instances of lack of antecedent basis and other matters of clarity in the claim language.

Applicants have amended each of these claims in accordance with the Examiner's suggestions so as to remove any instances of lack of antecedent basis and to avoid any instances of lack of clarity, and respectfully request that these rejections under 35 U.S.C. § 112 be withdrawn.

In paragraph 23 of the Office Action the Examiner has rejected claim 1 under 35 U.S.C. § 102(e) as being anticipated by Davis (U.S. Patent No. 6,058,478). In paragraph 24 of the Office Action, the Examiner has rejected claims 20 and 21 under 35 U.S.C. § 102(e) as being anticipated by Spies et al. (U.S. Reissue Patent No. RE38070). In paragraph 25 of the Office Action the Examiner has rejected claims 2-6, 9-12, 15-19 and 22 under 35 USC § 103(a) as being unpatenable over Spies in view of Davis. The Examiner has noted in paragraph 27 that claims 7, 8 13 and 14 are allowable if re-written to overcome the rejections set forth under 35 U.S.C. § 112.

Applicants respectfully disagree with the Examiner's contentions and submit the following remarks in response.

Regarding the first prior art rejection, the present invention as claimed in claim 1 is directed to a cryptographic communication method wherein *when different encryption algorithms are operated at a transmission side and a reception side*, the transmission side encrypts an encryption algorithm operated at the transmission side with an encryption algorithm operated at the reception side and transmits the encrypted algorithm to the reception side.

The cited prior art, namely, Davis, discloses an upgrading method which generates an upgrade message, which is encrypted with a public key of the message receiver and then sent to a remote device. The remote device then upgrades the message including the encryption algorithms. The method for this operation is set forth in the Davis patent in claims 5, 6 and 8. Such an invention is intended to both to allow for updating encryption algorithms and to allow upgrades of encryption keys, for example from 40-bit keys to 56-bit keys as government regulations or other such factors change over time.

However, there is no teaching or suggestion in Davis that discloses the present invention as claimed. For Example, there is no teaching or suggestion in Davis that discloses a cryptographic communication method where when different encryption algorithms are operated at a transmission side and a reception side, the transmission side *encrypts an encryption algorithm operated at the transmission side with an encryption algorithm operated at the reception side and transmits the encrypted algorithm to the reception side.* Thus, Applicants respectfully request that the rejection of claim 1 in view of Davis be withdrawn.

Regarding the second rejection, claim 20 of the present invention is directed to an encryption algorithm sharing management method for sharing an encryption algorithm

for cryptographic communication, comprising the steps of obtaining from a user of a transmission side, a user identifier indicating the user of the transmission side and a user identifier indicating a user of a reception side. A data base is queried in which user identifiers indicating users and corresponding encryption algorithms are preliminarily described so as to obtain an encryption algorithm, operable by the user of the transmission side, and an encryption algorithm operable by the user of the reception side.

It is then determined whether or not there is an encryption algorithm operable by the user of the transmission side and the user of the reception side commonly. If the commonly operable encryption algorithm exists, the user of the transmission side is notified that cryptographic communication at the user of the transmission side and the user of the reception side is enabled.

In this configuration, the algorithm sharing management method of the present invention is able to communicate to and notify the user on the transmission side whether or not a commonly operable encryption algorithm exists between the transmission side and the reception side.

The cited prior art, namely Spies, is directed to a system of tri-level architecture for securing a users' encryption keys in a multi-layered encryption system. In particular, in columns 15-17, cited by the Examiner, a method is described for selecting the encryption algorithm between two communicating entities. In column 15, lines 52-58 Spies states:

> "When an originating participant encrypts a document or instrument for a specific recipient, that originating participant takes his or her encryption index, along with the encryption index of the intended recipient, and uses the two values to look up the appropriate algorithm in a

preestablished table. This table typically is established by the certifying authority for the version of the commerce protocol being used."

This table is used prior to communication and uses the values to "look up" the appropriate algorithm on the pre-established table. The communication data structure, illustrated in Fig. 9, is then used after an encryption is selected from the table, using a tag-length-value data structure, in order to carry the packages exchanged between the participants.

Such an arrangement is not analogous to the present invention, because there is no *notification* delivered to the user of the transmission side, but rather Spies simply maintains a pre-existing column which table which is unable to dynamically confirm the existence of a commonly operable encryption algorithm.

As such, there is no teaching or suggestion in Spies that discloses the present invention as claimed. For example, there is no teaching or suggestion in Spies that discloses that when a commonly operable encryption algorithm exists, *the user of the transmission side is notified* that cryptographic communication at the user of the transmission side and the user of the reception side is enabled. Thus Applicants respectfully request that the rejection of independent claim 20 be withdrawn. Dependent claim 21 is allowable for the same reasons.

Regarding the third rejection, Applicants respectfully submit that neither Davis nor Spies, either alone or in combination, teach or suggest the present invention as claimed, for the reasons set forth above. And, even if the references were combined, the resulting systems and methods, would still not teach all of the elements of the claims.

Furthermore, regarding claims 6 and 12, the present invention relates to an

arrangement where data, indicating the encryption algorithm operated by the user of the transmission side and an encryption key, corresponding to a key length of the encryption algorithm operated by the user of the transmission side, is encrypted with the encryption algorithm operated by the user of the reception side.

The Examiner has cited to lines 18-25 in column 2 of Davis to illustrate the basis of the rejection of these claims. However, such an element is not present in Davis. Rather, Davis merely states that cryptographic algorithms could be modified to upgrade the cryptographic device, but makes no mention of the specific use of data that indicates the encryption algorithm, operated by the user of the transmission side and an encryption key, corresponding to a key length of the encryption algorithm operated by the user of the transmission side, to be encrypted with the encryption algorithm operated by the user of the reception side. Thus, Applicants respectfully request that the all of the rejections of claims 2-6, 9-12, 15-19 and 22 be withdrawn.

As such, Applicants respectfully submit that the present invention as claimed is now in condition for allowance, the earliest possible notice of which is earnestly solicited. If the Examiner feels that a telephone interview would advance the prosecution of this application he is invited to contact the undersigned at the number listed below.

Respectfully submitted

SOFER & HAROUN, LLP

Dated: 11/3/03

By: _____

Joseph Sofer
Reg. No. 34, 438
317 Madison Avenue
Suite 910
New York, New York 10017
(212)697-2800